FIG. 1

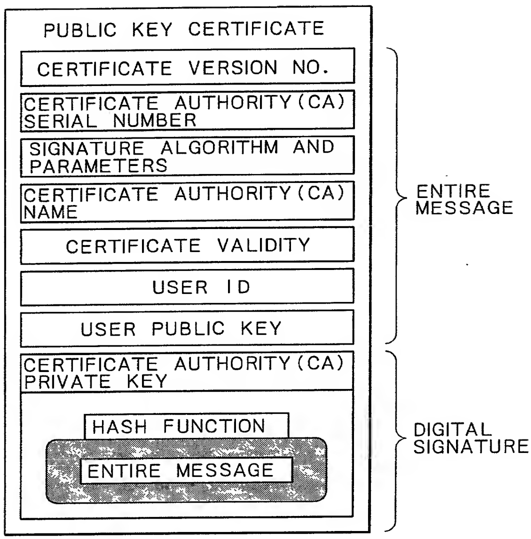

PUBLIC KEY CERTIFICATE
CERTIFICATE VERSION NO.
CERTIFICATE AUTHORITY (CA) SERIAL NUMBER
SIGNATURE ALGORITHM AND PARAMETERS
CERTIFICATE AUTHORITY (CA) NAME
CERTIFICATE VALIDITY
USER ID
USER PUBLIC KEY
CERTIFICATE AUTHORITY (CA) PRIVATE KEY
HASH FUNCTION
ENTIRE MESSAGE
ENTIRE MESSAGE
DIGITAL SIGNATURE

FIG. 2

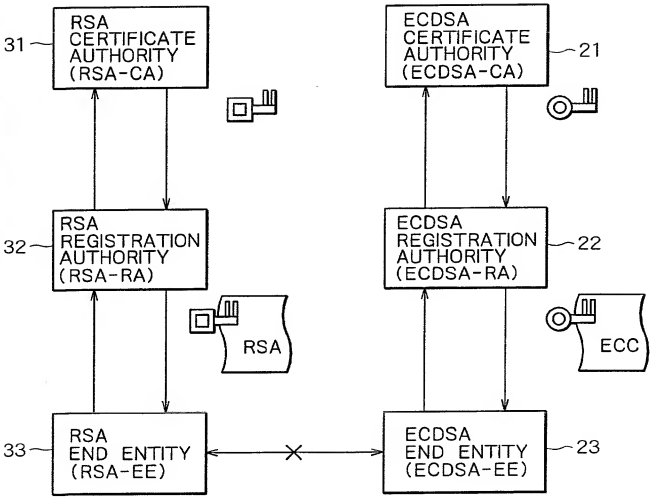

31
RSA CERTIFICATE AUTHORITY (RSA-CA)
ECDSA CERTIFICATE AUTHORITY (ECDSA-CA)
21
32
RSA REGISTRATION AUTHORITY (RSA-RA)
ECDSA REGISTRATION AUTHORITY (ECDSA-RA)
22
RSA
ECC
33
RSA END ENTITY (RSA-EE)
ECDSA END ENTITY (ECDSA-EE)
23

FIG. 3

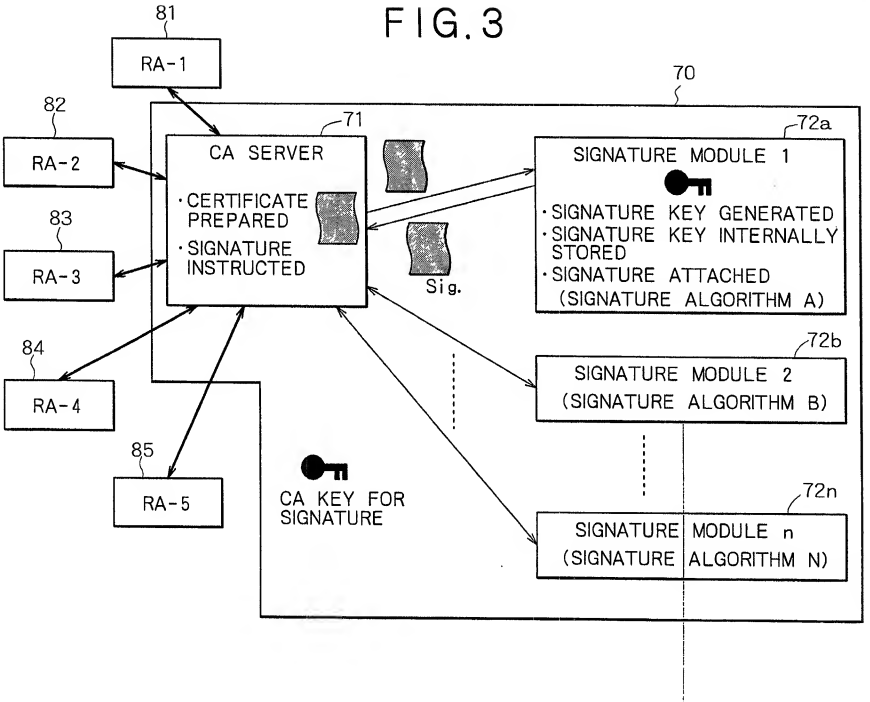

81
RA-1
70
82
RA-2
71
CA SERVER
72a
SIGNATURE MODULE 1
·CERTIFICATE PREPARED
·SIGNATURE INSTRUCTED
·SIGNATURE KEY GENERATED
·SIGNATURE KEY INTERNALLY STORED
·SIGNATURE ATTACHED (SIGNATURE ALGORITHM A)
83
RA-3
Sig.
84
RA-4
72b
SIGNATURE MODULE 2 (SIGNATURE ALGORITHM B)
85
RA-5
CA KEY FOR SIGNATURE
72n
SIGNATURE MODULE n (SIGNATURE ALGORITHM N)

FIG.4

EXAMPLE OF CERTIFICATE FORMAT (BASED ON X.509 V3)

ITEMS	DESCRIPTION	SETTINGS WITH THIS IA
Version 1		
version	VERSION OF CERTIFICATE FORMAT	V3
serial Number	CERTIFICATE SERIAL NUMBER FURNISHED BY IA	SEQUENTIAL SERIAL NUMBER
signature.algorithm Identifier algorithm parameters	CERTIFICATE SIGNATURE ALGORITHM AND PARAMETERS	·ELLIPTIC CURVE CRYPTOGRAPHY OR RSA ·PARAMETERS IN THE CASE OF ELLIPTIC CURVE CRYPTOGRAPHY ·KEY LENGTH IN THE CASE OF RSA
issuer	IA NAME (DISTINGUISHED NAME FORMAT)	NAME OF THIS IA
validity notBefore notAfter	VALIDITY OF CERTIFICATE ·STARTING DATE AND TIME ·ENDING DATE AND TIME	
subject	USER IDENTIFICATION NAME	USER DEVICE ID OR SERVICE ENTITY ID
subject Public Key Info algorithm subject Public key	USER'S PUBLIC KEY INFORMATION ·KEY ALGORITHM ·PUBLIC KEY	·ELLIPTIC CURVE CRYPTOGRAPHY OR RSA ·USER'S PUBLIC KEY
Version 3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	·KEY IDENTIFIER FOR SIGNATURE VERIFICATION BY IA ·KEY ID NUMBER (OCTAL) ·IA NAME (GENERAL NAME FORMAT) ·CERTIFICATE SERIAL NUMBER	
subject key Identifier	APPLICABLE WHERE MULTIPLE KEYS NEED TO BE CERTIFIED	NOT USED
key usage (0) digital Signature (1) non Repudiation (2) key Encipherment (3) data Encipherment (4) key Agreement (5) key CertSign (6) cRL Sign	THE PURPOSE OF KEY USAGE IS DESIGNATED (0) FOR DIGITAL SIGNATURE (1) FOR REPUDIATION PREVENTION (2) FOR KEY ENCRYPTION (3) FOR MESSAGE ENCRYPTION (4) FOR DISTRIBUTION OF COMMON KEY (5) FOR VERIFICATION OF SIGNATURE ON CERTIFICATE (6) FOR VERIFICATION OF SIGNATURE ON CERTIFICATE REVOCATION LIST	USAGE (0), (1), (4) AND (6) APPLY
private Key Usage Period notBefore notAfter	USAGE PERIOD OF USER'S PRIVATE KEY	USAGE PERIOD OF CERTIFICATE=USAGE PERIOD OF PUBLIC KEY=USAGE PERIOD OF PRIVATE KEY (DEFAULT)

FIG. 5

policy Mappings issuer Domain Policy subject Domain Policy	NECESSARY ONLY WHEN CA IS CERTIFIED. AN ISSUER DOMAIN POLICY AND A SUBJECT DOMAIN POLICY ARE DEFINED.	NONE BY DEFAULT
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ATTRIBUTES OF THE DIRECTORY (X.500) ARE DEFINED. WHEN THE OPPOSITE PARTY OF COMMUNICATION IS TO USE DIRECTORY INFORMATION, THAT PARTY IS INFORMED OF THE DIRECTORY ATTRIBUTES IN ADVANCE.	NONE BY DEFAULT
subject Alt Name	USER'S ALTERNATIVE NAME (GENERAL NAME FORMAT).	NOT USED
issuer Alt Name	THIS FIELD IS INCLUDED (NONE BY DEFAULT).	NONE BY DEFAULT
subject Directory Attributes	USER'S ANY ATTRIBUTES.	NOT USED
basic Constraints cA path Len Constraint	THIS FIELD SPECIFIES WHETER THE PUBLIC KEY SUBJECT TO CERTIFICATION IS TO BE SIGNED BY THE CERTIFICATE AUTHORITY (CA) OR USED BY THE USER.	USED BY USER BY DEFAULT
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	USED ONLY WHEN THE SUBJECT IS CA (CA CERTIFICATION).	NONE BY DEFAULT
policy Constraints require Explicit Policy inhibit Policy Mapping	DESCRIBED HERE ARE CONSTRAINTS REQUIRING EXPLICIT POLICY IDs AND INHIBIT POLICY MAPPING FOR THE REMAINING CERTIFICATION PATHS.	
CRL Distribution Points	DESCRIBED HERE ARE POINTS AT WHICH THE USER REFERENCES THE CERTIFICATE REVOCATION LIST (CRL) TO SEE WHETHER THE CERTIFICATE IS REVOKED.	THESE POINTS SERVE AS POINTERS INDICATING WHERE THE CERTIFICATE IS REGISTERED. THE CERTIFICATE REVOCATION LIST IS MANAGED BY THE ISSUER.
SIGNATURE	ISSUER'S SIGNATURE	

FIG. 6

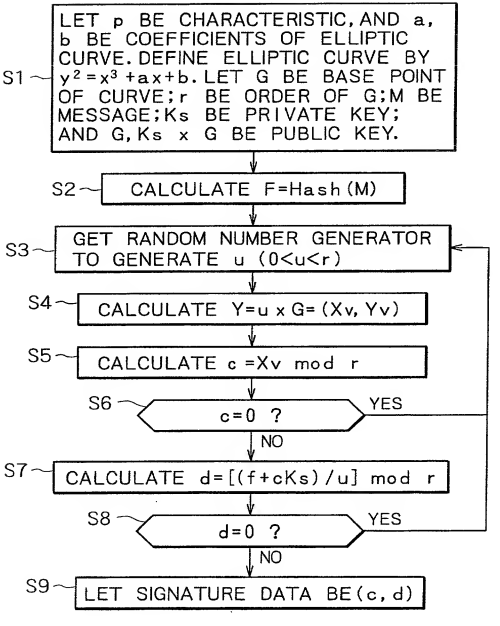

S1
LET p BE CHARACTERISTIC, AND a, b BE COEFFICIENTS OF ELLIPTIC CURVE. DEFINE ELLIPTIC CURVE BY $y^2=x^3+ax+b$. LET G BE BASE POINT OF CURVE; r BE ORDER OF G; M BE MESSAGE; Ks BE PRIVATE KEY; AND G, Ks x G BE PUBLIC KEY.
S2
CALCULATE F=Hash(M)
S3
GET RANDOM NUMBER GENERATOR TO GENERATE u (0<u<r)
S4
CALCULATE Y=u x G=(Xv, Yv)
S5
CALCULATE c=Xv mod r
S6
c=0 ?
YES
NO
S7
CALCULATE d=[(f+cKs)/u] mod r
S8
d=0 ?
YES
NO
S9
LET SIGNATURE DATA BE(c, d)

FIG. 7

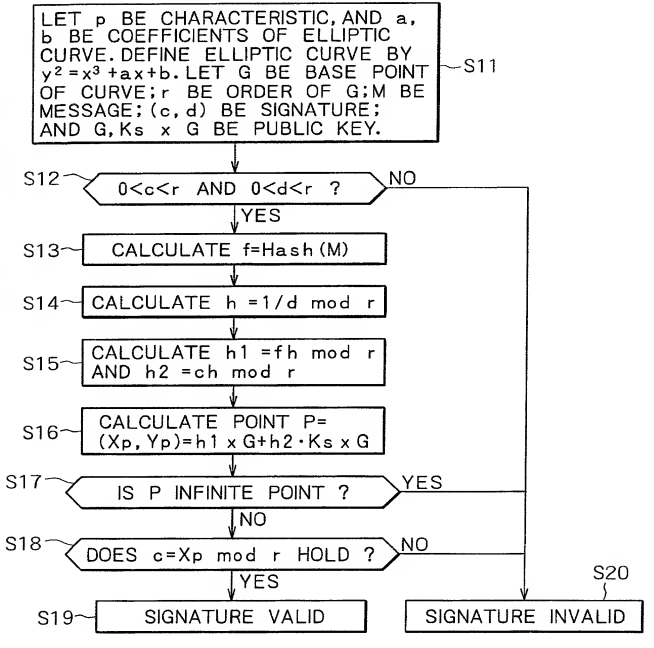

LET p BE CHARACTERISTIC, AND a, b BE COEFFICIENTS OF ELLIPTIC CURVE. DEFINE ELLIPTIC CURVE BY $y^2 = x^3 + ax + b$. LET G BE BASE POINT OF CURVE; r BE ORDER OF G; M BE MESSAGE; (c, d) BE SIGNATURE; AND G, Ks x G BE PUBLIC KEY.
S11
S12
0<c<r AND 0<d<r ?
NO
YES
S13
CALCULATE f=Hash(M)
S14
CALCULATE h =1/d mod r
S15
CALCULATE h1 =fh mod r AND h2 =ch mod r
S16
CALCULATE POINT P= (Xp, Yp)=h1 x G+h2·Ks x G
S17
IS P INFINITE POINT ?
YES
NO
S18
DOES c=Xp mod r HOLD ?
NO
YES
S19
SIGNATURE VALID
S20
SIGNATURE INVALID

FIG. 8

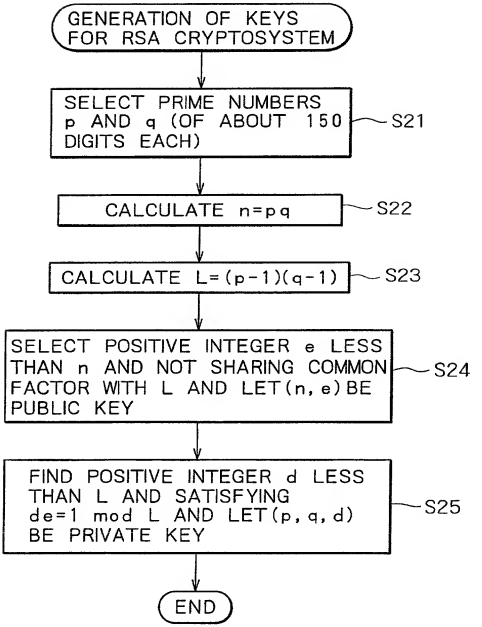

GENERATION OF KEYS FOR RSA CRYPTOSYSTEM
SELECT PRIME NUMBERS p AND q (OF ABOUT 150 DIGITS EACH)
S21
CALCULATE n=pq
S22
CALCULATE L=(p-1)(q-1)
S23
SELECT POSITIVE INTEGER e LESS THAN n AND NOT SHARING COMMON FACTOR WITH L AND LET(n, e) BE PUBLIC KEY
S24
FIND POSITIVE INTEGER d LESS THAN L AND SATISFYING de=1 mod L AND LET(p, q, d) BE PRIVATE KEY
S25
END

FIG. 9A

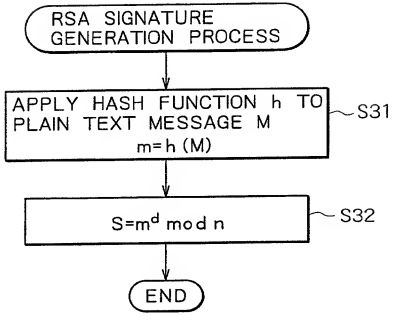


FIG. 9B

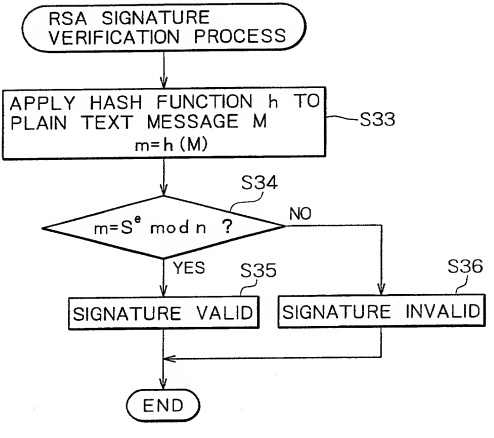


FIG. 10

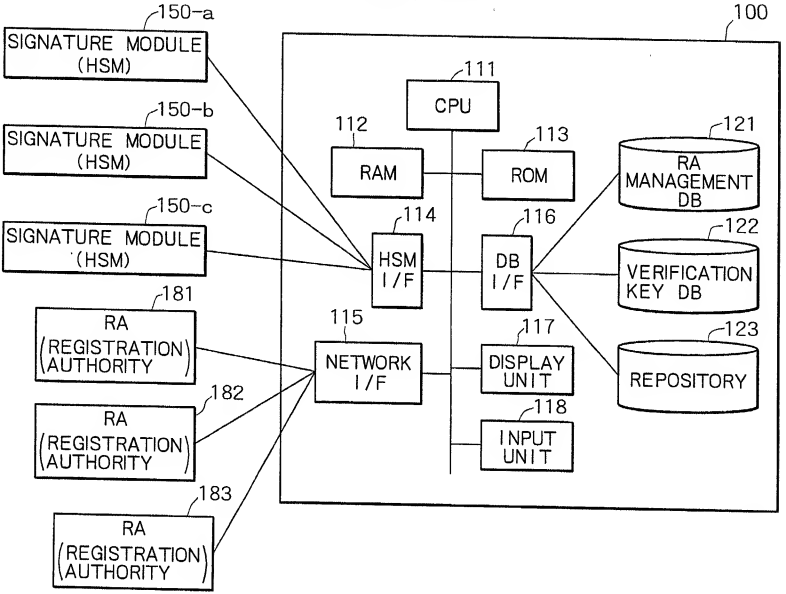


FIG. 11

EXAMPLE OF RA MANAGEMENT DATABASE AT CA

RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA0001	×	RSA	1024 bits	—	×	001
RA0002	×	RSA	2048 bits	—	○	002, 003, 004
RA0003	○	RSA	512 bits	—	×	005
RA0003	○	ECDSA	160 bits	p=XX,...	×	101
RA0004	○	RSA	1024 bits	—	×	006
RA0004	○	RSA	2048 bits	—	×	007
RA0004	○	ECDSA	192 bits	p=YY,...	×	102
RA0004	○	ECDSA	224 bits	p=ZZ,...	×	103

FIG. 12

VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
201	RSA	2048 bits	—	◇
201	RSA	1024 bits	—	◆
202	ECDSA	160 bits	p=XX,...	△
202	ECDSA	192 bits	p=YY,...	▲

FIG. 13

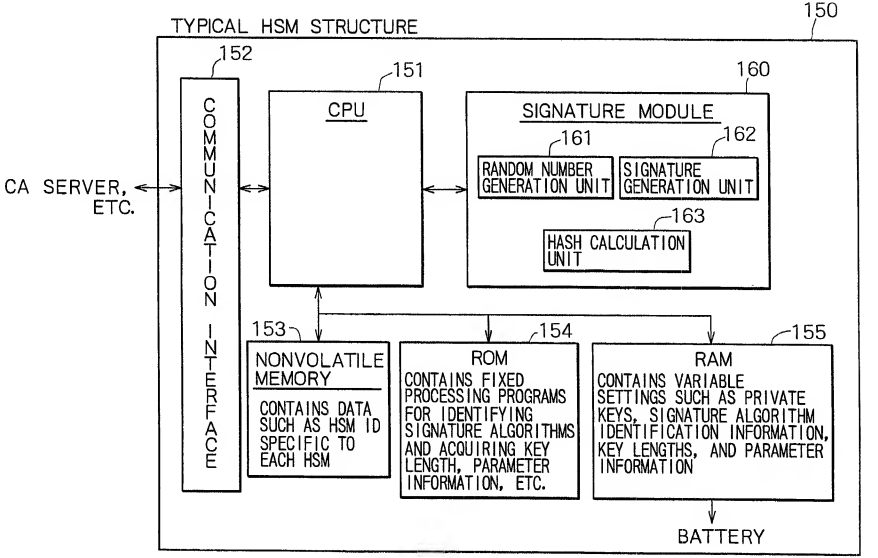

TYPICAL HSM STRUCTURE
150
152
COMMUNICATION INTERFACE
151
CPU
160
SIGNATURE MODULE
161
RANDOM NUMBER GENERATION UNIT
162
SIGNATURE GENERATION UNIT
163
HASH CALCULATION UNIT
CA SERVER, ETC.
153
NONVOLATILE MEMORY
CONTAINS DATA SUCH AS HSM ID SPECIFIC TO EACH HSM
154
ROM
CONTAINS FIXED PROCESSING PROGRAMS FOR IDENTIFYING SIGNATURE ALGORITHMS AND ACQUIRING KEY LENGTH, PARAMETER INFORMATION, ETC.
155
RAM
CONTAINS VARIABLE SETTINGS SUCH AS PRIVATE KEYS, SIGNATURE ALGORITHM IDENTIFICATION INFORMATION, KEY LENGTHS, AND PARAMETER INFORMATION
BATTERY

FIG.14

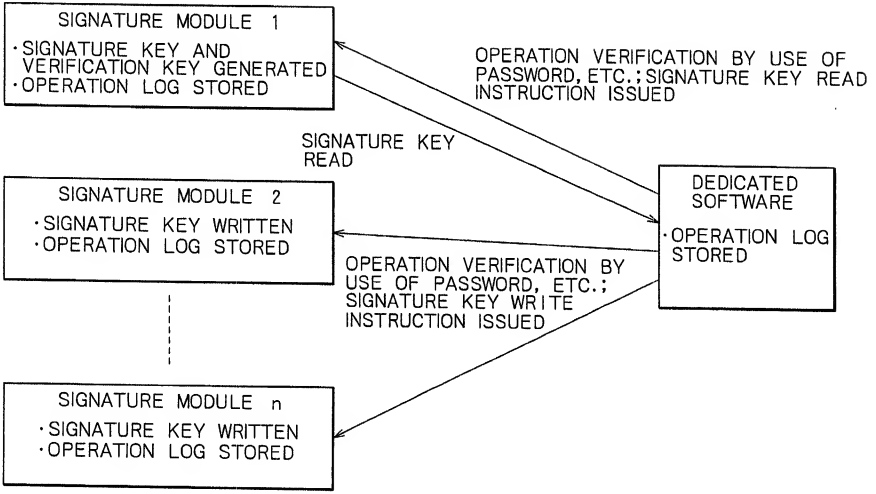

SIGNATURE MODULE 1
·SIGNATURE KEY AND VERIFICATION KEY GENERATED
·OPERATION LOG STORED
OPERATION VERIFICATION BY USE OF PASSWORD, ETC.; SIGNATURE KEY READ INSTRUCTION ISSUED
SIGNATURE KEY READ
SIGNATURE MODULE 2
·SIGNATURE KEY WRITTEN
·OPERATION LOG STORED
DEDICATED SOFTWARE
·OPERATION LOG STORED
OPERATION VERIFICATION BY USE OF PASSWORD, ETC.; SIGNATURE KEY WRITE INSTRUCTION ISSUED
SIGNATURE MODULE n
·SIGNATURE KEY WRITTEN
·OPERATION LOG STORED

FIG. 15

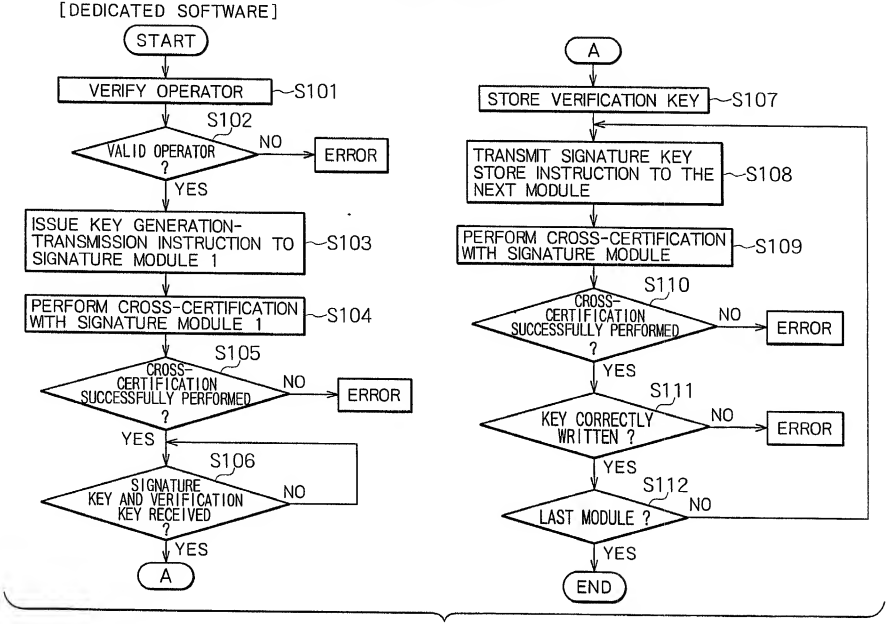


FIG. 16

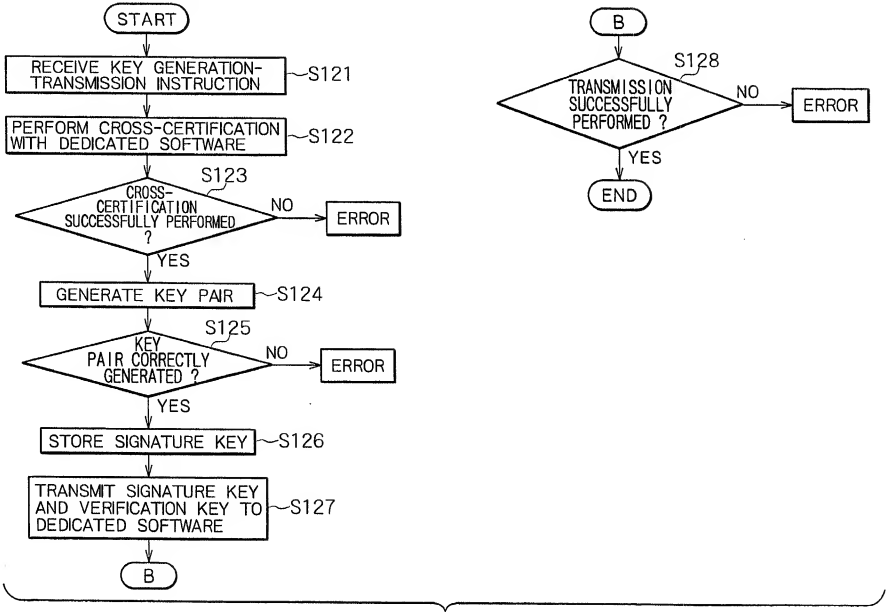

[SIGNATURE MODULE 1]
START
RECEIVE KEY GENERATION-TRANSMISSION INSTRUCTION
S121
PERFORM CROSS-CERTIFICATION WITH DEDICATED SOFTWARE
S122
S123
CROSS-CERTIFICATION SUCCESSFULLY PERFORMED ?
NO
ERROR
YES
GENERATE KEY PAIR
S124
S125
KEY PAIR CORRECTLY GENERATED ?
NO
ERROR
YES
STORE SIGNATURE KEY
S126
TRANSMIT SIGNATURE KEY AND VERIFICATION KEY TO DEDICATED SOFTWARE
S127
B
B
S128
TRANSMISSION SUCCESSFULLY PERFORMED ?
NO
ERROR
YES
END

FIG. 17

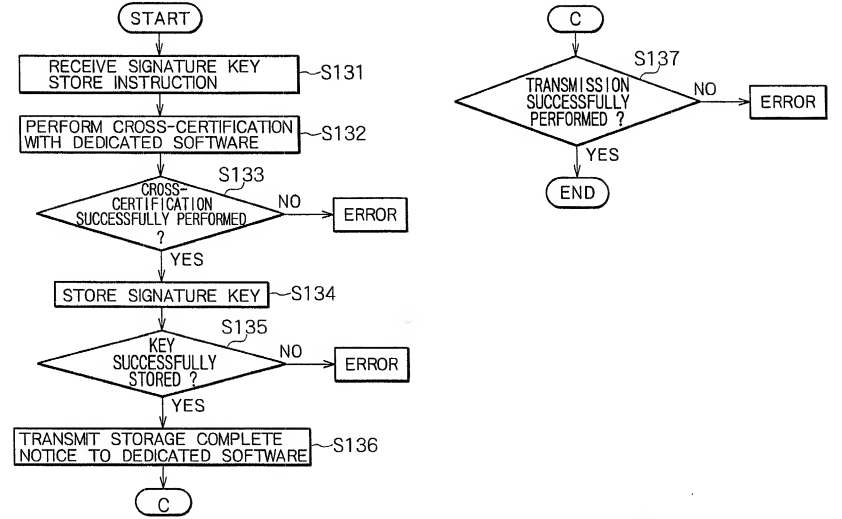

[SIGNATURE MODULE 2 THROUGH N]
START
RECEIVE SIGNATURE KEY STORE INSTRUCTION
S131
PERFORM CROSS-CERTIFICATION WITH DEDICATED SOFTWARE
S132
S133
CROSS-CERTIFICATION SUCCESSFULLY PERFORMED ?
NO
ERROR
YES
STORE SIGNATURE KEY
S134
S135
KEY SUCCESSFULLY STORED ?
NO
ERROR
YES
TRANSMIT STORAGE COMPLETE NOTICE TO DEDICATED SOFTWARE
S136
C
C
S137
TRANSMISSION SUCCESSFULLY PERFORMED ?
NO
ERROR
YES
END

FIG. 18

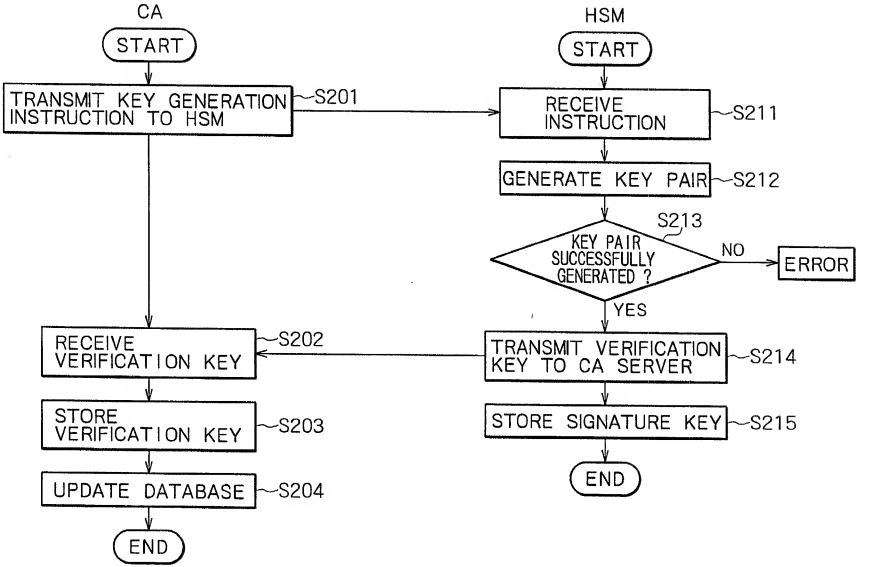

CA
START
TRANSMIT KEY GENERATION INSTRUCTION TO HSM
S201
RECEIVE VERIFICATION KEY
S202
STORE VERIFICATION KEY
S203
UPDATE DATABASE
S204
END
HSM
START
RECEIVE INSTRUCTION
S211
GENERATE KEY PAIR
S212
S213
KEY PAIR SUCCESSFULLY GENERATED ?
NO
ERROR
YES
TRANSMIT VERIFICATION KEY TO CA SERVER
S214
STORE SIGNATURE KEY
S215
END

FIG. 19

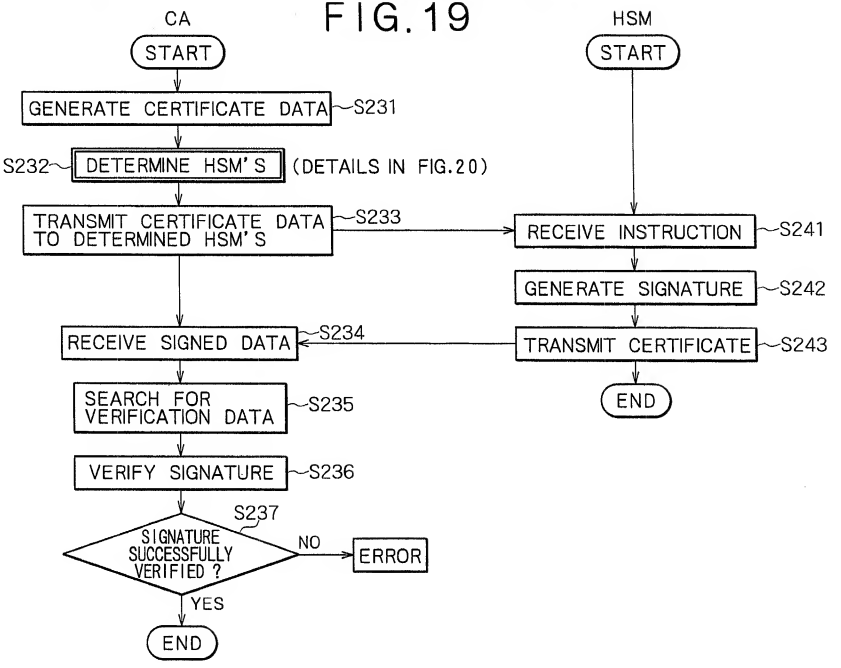


FIG. 20

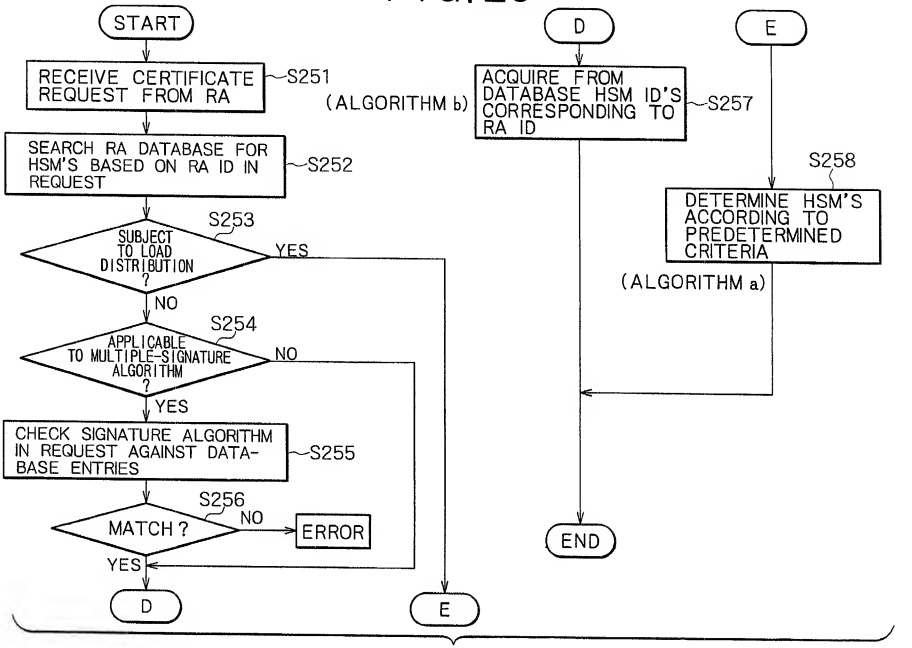
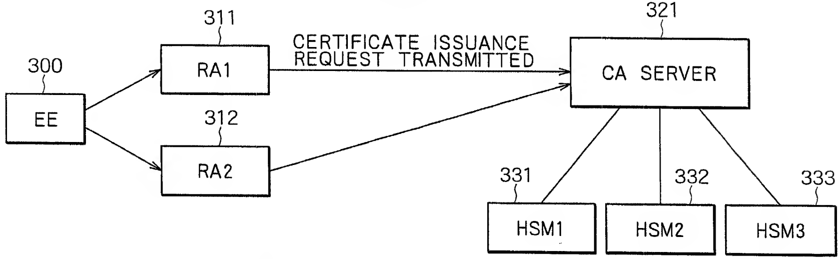

CA
START
RECEIVE CERTIFICATE REQUEST FROM RA
S251
SEARCH RA DATABASE FOR HSM'S BASED ON RA ID IN REQUEST
S252
S253
SUBJECT TO LOAD DISTRIBUTION ?
YES
NO
S254
APPLICABLE TO MULTIPLE-SIGNATURE ALGORITHM ?
NO
YES
CHECK SIGNATURE ALGORITHM IN REQUEST AGAINST DATA-BASE ENTRIES
S255
S256
MATCH ?
NO
ERROR
YES
D
E
D
ACQUIRE FROM DATABASE HSM ID'S CORRESPONDING TO RA ID
S257
(ALGORITHM b)
END
E
S258
DETERMINE HSM'S ACCORDING TO PREDETERMINED CRITERIA
(ALGORITHM a)

FIG. 21



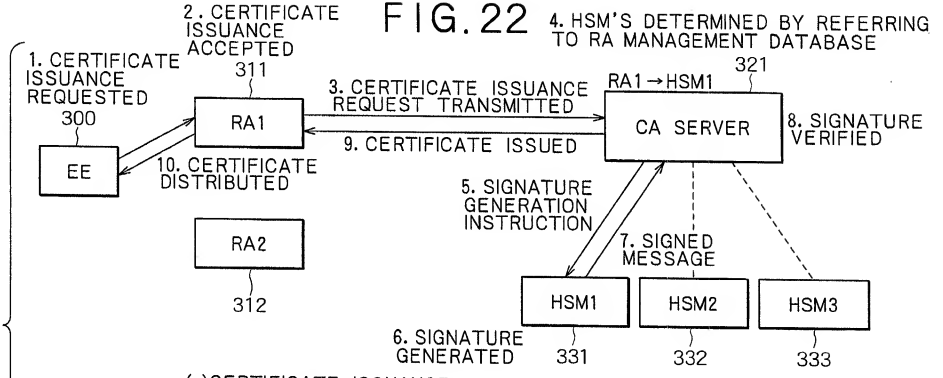
(a) RA MANAGEMENT DATABASE

RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA1	×	RSA	1024 bits	—	×	HSM1
RA2	○	RSA	2048 bits	—	×	HSM2
RA2	○	ECDSA	192 bits	p=XX,…	×	HSM3
RA2	○	ECDSA	192 bits	p=YY,…	×	HSM3

(b) VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
HSM1	RSA	1024 bits	—	◇
HSM2	RSA	2048 bits	—	◆
HSM3	ECDSA	192 bits	p=XX,…	△
HSM3	ECDSA	192 bits	p=YY,…	▲

FIG. 22



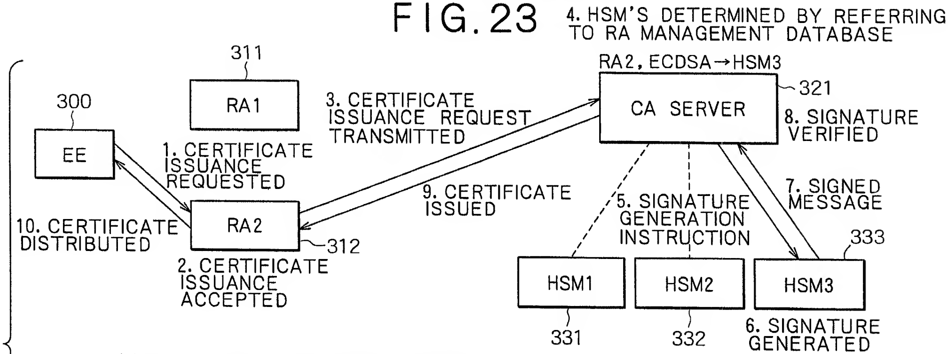
(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID
CERTIFICATE ISSUANCE	Message1	RA2

(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE
SIGNATURE GENERATION	Message1

FIG. 23



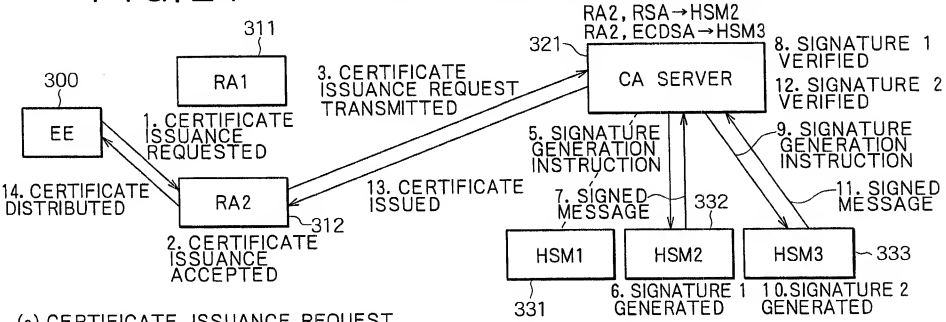
(a)CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNAL ALGORITHM	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message2	RA2	ECDSA	192 bits	p=XX,...

(b)SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message2	192 bits	p=XX,...

FIG. 24



(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNATURE ALGORITHM 1	KEY LENGTH	SIGNATURE ALGORITHM 2	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message3	RA2	RSA	2048 bits	ECDSA	192 bits	p=XX,...

(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH
SIGNATURE GENERATION	Message3	2048 bits

(c) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message3	192 bits	p=YY,...

FIG. 25

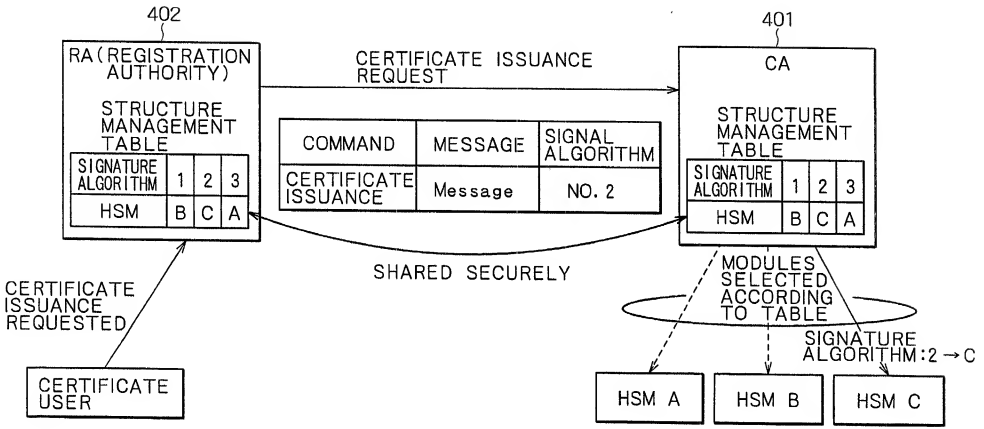
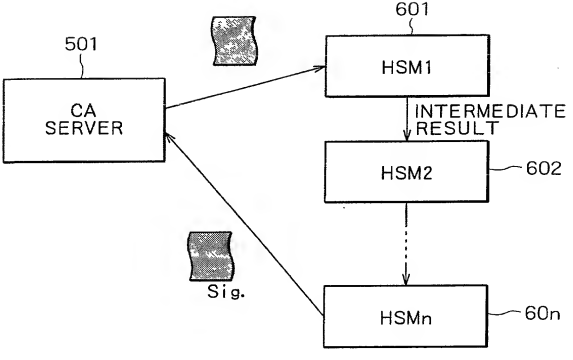


FIG. 26


601
501
HSM1
CA
SERVER
INTERMEDIATE
RESULT
HSM2
602
Sig.
HSMn
60n